ORIGINAL

Approved: ______________________________
SIDHARDHA KAMARAJU / ANDREW K. CHAN
Assistant United States Attorneys

Before: HONORABLE DEBRA FREEMAN
Chief United States Magistrate Judge
Southern District of New York

DOC #

17 MAG 1389

UNITED STATES OF AMERICA	**SEALED COMPLAINT**
- v. -	Violations of 18 U.S.C. §§ 1030(a)(2)(C), (a)(4), (C)(2)(B), and 2.
KEVIN FORBES,	
Defendant.	COUNTY OF OFFENSE: NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

EVELINA ASLANYAN, being duly sworn, deposes and says that she is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE

1. On or about February 23, 2017, in the Southern District of New York and elsewhere, KEVIN FORBES, the defendant, intentionally accessed a computer without authorization and exceeded authorized access and thereby obtained information from a protected computer, which offense was committed for purposes of commercial advantage and private financial gain, and the value of the information obtained exceeded $5,000, to wit, FORBES used the login credentials for an employee of a particular company ("Victim-1") to access a Victim-1 administrative page without authorization, and thereby obtained unauthorized access to information relating to resumes, subscribers, and employees of Victim-1.

(Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i), 1030(c)(2)(B)(iii), and 2).

COUNT TWO

2. On or about February 23, 2017, in the Southern District of New York and elsewhere, KEVIN FORBES, the defendant, knowingly and with intent to defraud, accessed a protected computer without authorization and exceeded authorized access and by means of such conduct, furthered the intended fraud and obtained something of value, to wit, FORBES accessed a Victim-1 administrative page without authorization with the intent to invite customers of Victim-1 to join a website controlled by FORBES.

(Title 18, United States Code, Sections 1030(a)(4) and 2).

The bases for my knowledge and for the foregoing charges are, in part, as follows:

3. I have been a Special Agent with the FBI for approximately five years. I am currently assigned to a squad responsible for investigating computer network intrusions. I have participated in investigations of such offenses, and have made and participated in arrests of individuals who have committed such offenses.

4. The information contained in this Complaint is based upon my personal knowledge, as well as information obtained during this investigation, directly or indirectly, from other sources, including, but not limited to: (a) business records and other documents, including records of electronic communications; (b) publicly available documents; (c) conversations with, and reports of interviews with, law enforcement and non-law-enforcement witnesses; (d) conversations with, and reports prepared by, other FBI agents; (e) documents provided by employees of Victim-1. Because this Complaint is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions and statements of and conversations with others are reported herein, they are reported in substance and in part. Where figures, calculations, and dates are set forth herein, they are approximate, unless stated otherwise.

Background

5. Several Internet-based businesses operate websites that serve as online job boards. Online job boards allow job-seekers to upload their resumes and apply for job openings posted on the websites by recruiting agencies[1] and employers. Similarly, recruiting agencies and employers can also solicit job-seekers directly for job opportunities through the website. For these reasons, the size of a given website's job-seeker database--and especially the number of resumes and jobs in the database--can make the website more attractive to job-seekers, recruiting agencies, and employers. An example of a prominent online job board is Monster.com.

6. Online job boards can generate revenue by selling advertising space on their website. The desirability and pricing of such space is driven, in part, by the number of users who visit the website and the number of page views by users. Online job boards can also generate revenue by offering premium accounts for a fee that allow additional services or functionality. For example, some online job boards will offer premium accounts to recruiters or employers, allowing them to post potential job opportunities or access the user database. Just as with advertising revenue, the size of a website's job-seeker database can have an impact on the revenues from premium accounts.

7. At all times relevant to this Complaint, Victim-1 was a publicly-traded company in the online job board industry headquartered in the United States. Victim-1 owns and maintains a website that is, among other things, an online job board for professionals working in the oil and gas industry ("Website-1"). Website-1 allows its members to create profiles, which include personal and professional information. As part of their profiles, members can also upload their resumes. The profiles are contained in a database maintained by Website-1 (the "Website-1 Resume Database").

8. Recruiting agencies and employers pay Website-1 for subscriptions, which allows them to view resumes and solicit job-seekers from the Website-1 Resume Database. Victim-1 maintains customer data for recruiters and employers who have paid for subscriptions, which includes, among other things, the

[1] A recruiting agency (sometimes also colloquially known as a "headhunter") is paid a commission by employers for finding qualified job applicants for open positions.

names of recruiters and employers, the price paid for access to the Website-1 Resume Database, the dates when the subscriptions with Website-1 began, the length of the subscription, and the terms of the subscription (the "Website-1 Customer Data"). Website-1 Customer Data is not publicly available.

FORBES's Illicit Access to the Website-1 Customer Data

9. Based on my participation in this investigation, my review of records, my review of publicly-available information, and my conversation with a confidential source (the "CS"),[2] I have learned the following:

a. KEVIN FORBES, the defendant, lives in Aberdeen, United Kingdom. Since in or around May 2009, FORBES has been the Managing Director of OilandGasPeople.com, which, like Victim-1, also operates an online job board in the oil and gas industry. OilandGasPeople.com maintains a resume database and solicits job-seekers to upload their resumes. FORBES is not employed by or otherwise associated with Victim-1 or Website-1.

b. Between in or around January 2017 and in or around February 2017, at the FBI's direction, the CS engaged in recorded conversations with FORBES. Based on my review of these recordings, it appears that FORBES reported to the CS that FORBES had accessed and downloaded a large quantity of resumes, email addresses, and customer data from an online job board in the oil and gas industry. FORBES also offered to sell to the CS a portion of this data for approximately $250,000.

c. On or about January 24, 2017, FORBES emailed to the CS links to download approximately 450,000 resumes (the "Stolen Resumes") and a spreadsheet containing customer data for approximately 800 customers (the "Stolen Customer Data"). The Stolen Resumes appeared to contain resumes associated with job-seekers located all around the world, including the United States. Similarly, the Stolen Customer Data appeared to contain information regarding Website-1 customers from all around the world, including the United States.

[2] The CS pleaded guilty to a computer fraud charge in late 2016 and began cooperating with the Government in early 2017 in hopes of obtaining a more lenient sentence. Information from the CS has been deemed reliable and has been corroborated by, among other things, recorded phone conversations and information received from Victim-1.

d. On or about February 1, 2017, a portion of the Stolen Customer Data was given to representatives of Victim-1, who confirmed that the Stolen Customer Data appeared to come from the Website-1 Customer Data. As a result, representatives of Victim-1 also believe that the Stolen Resumes came from the Website-1 Resume Database.

10. On or about February 23, 2017, at the FBI's direction, the CS participated in a meeting with KEVIN FORBES, the defendant, at a hotel in Manhattan, New York (the "February 23 Meeting"). An undercover FBI agent (the "UC") also participated in the February 23 Meeting. Based on my review of surveillance video and my conversations with the UC, I have learned that the following occurred during that meeting:

a. FORBES, the CS, and the UC discussed how the CS and FORBES could continue to obtain Stolen Resumes and Stolen Customer Data for a joint venture to create a new online job board in the oil and gas industry.

b. FORBES stated that he had "22 logins" with administrative access into Website-1. Based on my training, experience, and participation in this investigation, it appears that FORBES was indicating that he had twenty-two different credentials, which would afford him access to resumes, usernames, passwords, and other information associated with Website-1, which he was not, in fact, authorized to see.

c. The UC observed FORBES use a laptop computer to log into a virtual private network.[3] Once he had done so, the UC saw FORBES use login credentials that appeared to belong to an employee of Website-1 to access an administrative webpage associated with Website-1.

d. After FORBES had logged into Website-1, the UC observed that the screen contained various links to view information relating to resumes, subscribers, and employees who had uploaded information to Website-1. Among other things, FORBES accessed a webpage that appeared to provide a list of resumes that had been recently uploaded to Website-1. FORBES later stated, "You can get into every client account," while on a webpage that provided access to the usernames and passwords for subscribers of Website-1. Based on my training, experience, participation in this investigation, and conversations with the UC, it appears to me that FORBES was advising the UC and the CS

[3] A virtual private network is a service that allows a computer user to hide or mask their Internet Protocol address.

that, using his credentials, FORBES could illicitly access client information for all of Website-1's users.

WHEREFORE, I respectfully request that an arrest warrant be issued for KEVIN FORBES, the defendant, and that he be arrested and imprisoned or bailed, as the case may be.

EVELINA ASLANYAN
Special Agent
Federal Bureau of Investigation

Sworn to before me this
23rd day of February 2017

HONORABLE DEBRA FREEMAN
CHIEF UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK